IN THE CLAIMS:

Please amend claims 34 and 47 as follows:

1.   (Original) A method of controlling copying of an information signal in a system having a source of the information signal and a device for copying the information signal, the method comprising the steps of:

at an information signal modification source, prior to transmission of the information signal to the copying device, generating a copy control password and a related reference password, and applying to the information signal a substantially imperceptible modification representing copy control data including the copy control password securely encoded according to a predetermined algorithm;

delivering the modified information signal from the modification source to the copying device via a communications channel;

delivering the reference password from the modification source to the copying device via a separate communications channel independent of the modified information signal;

upon reception of the modified signal deriving the copy control data from the modified information signal;

comparing the derived securely encoded password with the separately provided reference password securely encoded according to a predetermined algorithm; and

enabling copying of the information signal if the securely encoded password derived from the information signal and the securely encoded reference password have a predetermined relationship.

2.   (Original) A method according to claim 1, wherein the reference password is securely encoded according to the same algorithm as the derived password.

3. (Original) A method according to claim 1, wherein the copy control data additionally includes other data indicating that copying is permitted if a correct reference password is provided.

4. (Original) A method according to claim 1, wherein the copy control password and the reference password are the same and the predetermined algorithm is a hash function.

5. (Original) A method according to claim 1, wherein the reference password is delivered to the copying device by the steps of providing the reference password to a user of the information signal who provides the reference password to the copying device.

6. (Original) A method according to claim 5, wherein the reference password is provided to the user if the user fulfils at least one predetermined condition.

7. (Original) A method according to claim 6, wherein the condition is payment for provision of the password.

8. (Original) A method according to claim 5, wherein the password is provided to the user via a secure communications channel.

9. (Original) A method according to claim 5, wherein the password is provided to the user on a secure data carrier.

10. (Original) A method according to claim 1, comprising the step of prompting the user to provide the password, the prompting of the user occurring in response to the derivation of the copy control data.

11. (Original) A method according to claim 1, comprising the step of storing the modified information signal on a data carrier for supply to the said user.

12. (Original) A method according to claim 1, wherein the modification is applied to the information signal by modifying transform coefficients of the information signal.

13. (Original) A method according to claim 12, wherein the said coefficients are DCT or Wavelet coefficients.

14. (Original) A method according to claim 1, wherein the information signal comprises any one or more of: image information, video information, audio information, text and data.

15. (Original) A system for controlling copying of an information signal the system having a source of the information signal and a device for copying the information signal and further comprising:

an information signal modification apparatus operable, prior to transmission of the information signal to the copying device, to generate a copy control password and a related reference password, and apply to the information signal a substantially imperceptible modification representing copy control data including the copy control password securely encoded according to a predetermined algorithm;

a communications channel for delivering the modified information signal from the modification source to the copying device; and

a separate communications channel independent of the modified information signal for delivering the reference password from the modification source to the i copying device; wherein

the copying device comprises a data processor and an input device for providing the reference password to the data processor, the data processor being operable to

a) derive the copy control data from the modified information signal upon reception of the modified signal, and

b) compare the derived securely encoded password with the separately provided reference password securely encoded according to a predetermined algorithm; and

c) a copying unit enabled by the data processor to copy the information signal if the securely encoded password derived from the information signal and the securely encoded reference password have a predetermined relationship.

16.   (Original) A system according to claim 15, wherein the data processor is arranged to securely encode the reference password according to the same algorithm as the derived password.

17.   (Original) A system according to claim 15, wherein the predetermined algorithm is a hash function.

18.   (Original) A system according to claim 15, wherein the input device is a keyboard.

19.   (Original) A system according to claim 15, wherein the input device is a reader for reading data from a data carrier.

20.   (Original) A system according to claim 15, wherein the input device comprises a communications interface for receiving the reference password from a communications network.

21.   (Original) A system according to claim 15, wherein the signal modification apparatus is operable to apply the modification by modifying transform coefficients of the information signal.

22.   (Original) A system according to claim 21, wherein the transform coefficients are DCT or Wavelet coefficients.

23.   (Original) A system according to claim 15, further comprising means for prompting a user to provide the reference password to the data processor via the input device.

24.   (Original) An information signal to which is applied a substantially imperceptible modification representing copy control data including a password securely encoded according to a predetermined algorithm and other data indicating that copying is permitted if a correct reference password is provided.

25. (Original) A signal according to claim 24, wherein the predetermined algorithm is a hash function.

26. (Original) A signal according to claim 24, wherein the modification is applied to the information signal by modifying transform coefficients of the information signal.

27. (Original) A signal according to claim 26, wherein the said coefficients are DCT or Wavelet coefficients.

28. (Original) A signal according to claim 24, which comprises any one or more of image information, video information, audio information, text and data.

29. (Original) A data carrier on which is recorded a signal according to claim 24.

30. (Original) A data carrier according to claim 29 which is a disc.

31. (Original) A signal modification apparatus operable to apply to an information signal a substantially imperceptible modification by modifying transform coefficients of the information signal, the modification representing copy control data including a password securely encoded according to a predetermined algorithm and other data indicating that copying is permitted if a correct reference password is provided.

32. (Original) Apparatus according to claim 31, wherein the predetermined algorithm is a hash function.

33. (Original) Apparatus according to claim 31, wherein the said coefficients are DCT or Wavelet coefficients.

34. (Currently Amended) ~~An information signal copying device~~ Processing apparatus for copying an information signal to which is applied a substantially imperceptible modification representing copy control data including a password securely encoded according to a predetermined algorithm, the copying device comprising:

a data processor operable to receive the modified information signal, and an input device for receiving a reference password separately from, and independently of, the modified information signal, and for providing the reference password to the data processor, the data processor being operable to

a) derive the copy control data from the modified information signal upon reception of the modified signal, and

b) compare the derived securely encoded password with the separately provided reference password securely encoded according to a predetermined algorithm; and

c) a copying unit enabled by the data processor to copy the information signal if the securely encoded password derived from the information signal and the securely encoded reference password have a predetermined relationship.

35.   (Original) A processing apparatus according to claim 34, wherein the data processor is arranged to securely encode the reference password according to the same algorithm as the derived password.

36.   (Original) A processing apparatus according to claim 34, wherein the predetermined algorithm is a hash function.

37.   (Original) A processing apparatus according to claim 34, wherein the input device is a keyboard.

38.   (Original) A processing apparatus according to claim 34, wherein the input device is a reader for reading data from a data carrier.

39.   (Original) A processing apparatus according to claim 34, wherein the input device comprises a communications interface for receiving the reference password from a communications network.

40.   (Original) A processing apparatus according to claim 34, further comprising means for prompting a user to provide the reference password via the input device.

41.   (Original) A method of applying copy control data to an information signal comprising the steps of:

determining whether copying of the information signal is allowed, not allowed or conditionally allowed; and

applying to the signal a substantially imperceptible modification representing copy control data, the copy control data comprising a copy status code of

a) first data if copying is allowed,

b) second data if copying is not allowed, and

c) third data if copying is conditionally allowed, the third data including at least a password securely encoded according to a predetermined algorithm.

42.   (Original) A method according to claim 41, wherein the third data also includes other data indicating that copying is allowed on provision of a reference password.

43.   (Original) A method according to claim 41, wherein the predetermined algorithm is a hash function.

44.   (Original) A method according to claim 41, wherein the modification is applied to the information signal by modifying transform coefficients of the information signal.

45.   (Original) A method according to claim 44, wherein the said coefficients are DCT or Wavelet coefficients.

46.   (Original) A method according to claim 41, wherein the information signal comprises any one or more of image information, video information, audio information, text and data.

47. (Currently Amended) A method of controlling the operation of a signal copying device having a recording unit controlled by a processor, the copying device being operable to record an information signal produced by the method of claim 41 ~~any one of claims 41 to 46~~, the method comprising the steps of:

using the processor to derive the copy control data from the information signal and to determine whether the control data is the first, second or third data and to

a) allow the recording unit to record if the first data is present in the information signal,

b) disable the recording unit if the second data is present in the information signal; and

c) allow the recording unit to record if the third data is present in the information signal and a reference password is provided which when securely encoded by a predetermined algorithm has a predetermined relationship to the said securely encoded password of the third data.

48. (Original) A method according to claim 47, comprising the step of securely encoding the reference password according to the same algorithm as the said password of the third data.

49. (Original) A method according to claim 48 wherein the algorithm is a hash function.

50. (Original) A method according to claim 47, comprising the step of providing the reference password to the processor separately from the information signal.

51. (Original) A method according to claim 50, comprising the step of providing the reference password to the processor via a user.

52. (Original) A method according to claim 51, further comprising the step of prompting the user to provide the reference password.

53   (Original) A method according to claim 52, comprising the step of prompting the user to provide the password, the prompting of the user occurring in response to the derivation of the third data.

54.   (Original) A method according to claim 47, which includes using the said processor to detect whether or not a substantially imperceptible modification representing the copy control data is present in the information signal and, if it is not present, producing data which controls the recording unit in a predetermined manner.

55.   (Original) A method according to claim 54, wherein the said processor produces the said first data allowing the recording unit to record if the copy control data is not present in the information signal.

56.   (Currently Amended) A method according to claim 47, ~~of recording an information signal according to claim 42~~ wherein the third data indicates a copy may be made on provision of a reference password and the copy includes an imperceptible modification representing copy control data defined by the third data and comprising the step of applying to the copy an imperceptible modification representing copy control data defined by the third data..

57.   (Original) A method according to claim 56, wherein the said modification applied to the copy is different from that of the original signal.

58.   (Original) Apparatus arranged to carry out the method of claim 41.

59.   (Original) Apparatus arranged to carry out the method of claim 47.

60.   (Original) A computer program which when run on a suitable processing system implements the method of claim 1.

61.   (Original) A computer program which when run on a suitable processing system implements the method of claim 41.

62.   (Original) A computer program which when run on a suitable processing system

implements the method of claim 47.